TÊN ĐỀ TÀI

Member

AGENDA

- Context
- Technology Trends
- Project Objectives (Scope & Out of Scope)
- Business Requirements & Non-Business Requirements
- Architectures (Function/Application/Data/Infrastructure/Security Architectures)
- Scenarios Demo

CONTEXT

- Try to find Paintpoints: Technology, Procedures, People
- Eg: NG-EPP (EPP/EDR)
  - Paintpoint 1: Visibility attacks (Can not Visibility detail attack techniques)
  - Paintpoint 2: Detection attacks (Many Detection Engine: AV, HIDS, FIM,.. And lack of observations whole attacks in MITRE ATT&CK)
  - Paintpoint 3: Response via alert / notification (Can not automatically response as isolating host, killing processes,..)
  - Paintpoint 4: Incident Processes is complicated.
  - Paintpoint 5: Difficult to utilize human resources

TECHNOLOGY TRENDS

- Focus on Security Trends
- Mapping a specific security trends that we select to painpoints (Technology, Procedures, People)
- Eg: NG-EPP (EPP/EDR)
  - Paintpoint 1: Visibility attacks → Unified Dashboard to see detail attacks
  - Paintpoint 2: Detection → Included Engines as AV, HIDS, FIM, Threat Intelligence
  - Paintpoint 3: Response via alert / notification
    - → Integrate with Security Agent to kill malicious process, isolate an infected Host,..
    - → Run Playbooks that we defined to execute some task to hunt before.
  - Paintpoint 4: Incident Processes is complicated.
    - → Unified Dashboard to manage Incident
    - → Hunting Root-cause by playbooks
  - Paintpoint 5: Difficult to utilize human resources
    - → Optimize Security Tier 2/Tier3

PROJECT OBJECTIVES

- Objective 1: Completed Visibility & Detect Attack base on MITRE ATT&CK
- Objective 2: Deeply building up playbook to Response & Hunting
- Objective 3: Building up Incident Response Plan
- Objective 4: Showing Human Resources Optimization
- Objective 5: Research & Build virtual lab to demonstrate technical features

REQUITEMENT (BUSINESS & NON-BUSINESS)

No.	Business requirements	
1	Visibility attack	
2	Detect attack	
3	Response attack	
4	Hunt attack	
5	Incident Procedure	
6	Human Resource Optimization	

REQUITEMENT (BUSINESS & NON-BUSINESS)

No.	Non-Business requirements	
1	Business Volume: - Users: Y1, Y2, Y3 - Concurrence users: Y1, Y2, Y3	
2	Define: - RTO - RPO	
3	Backup & Restore	
4	Computing & Storage: Y1, Y2, Y3	